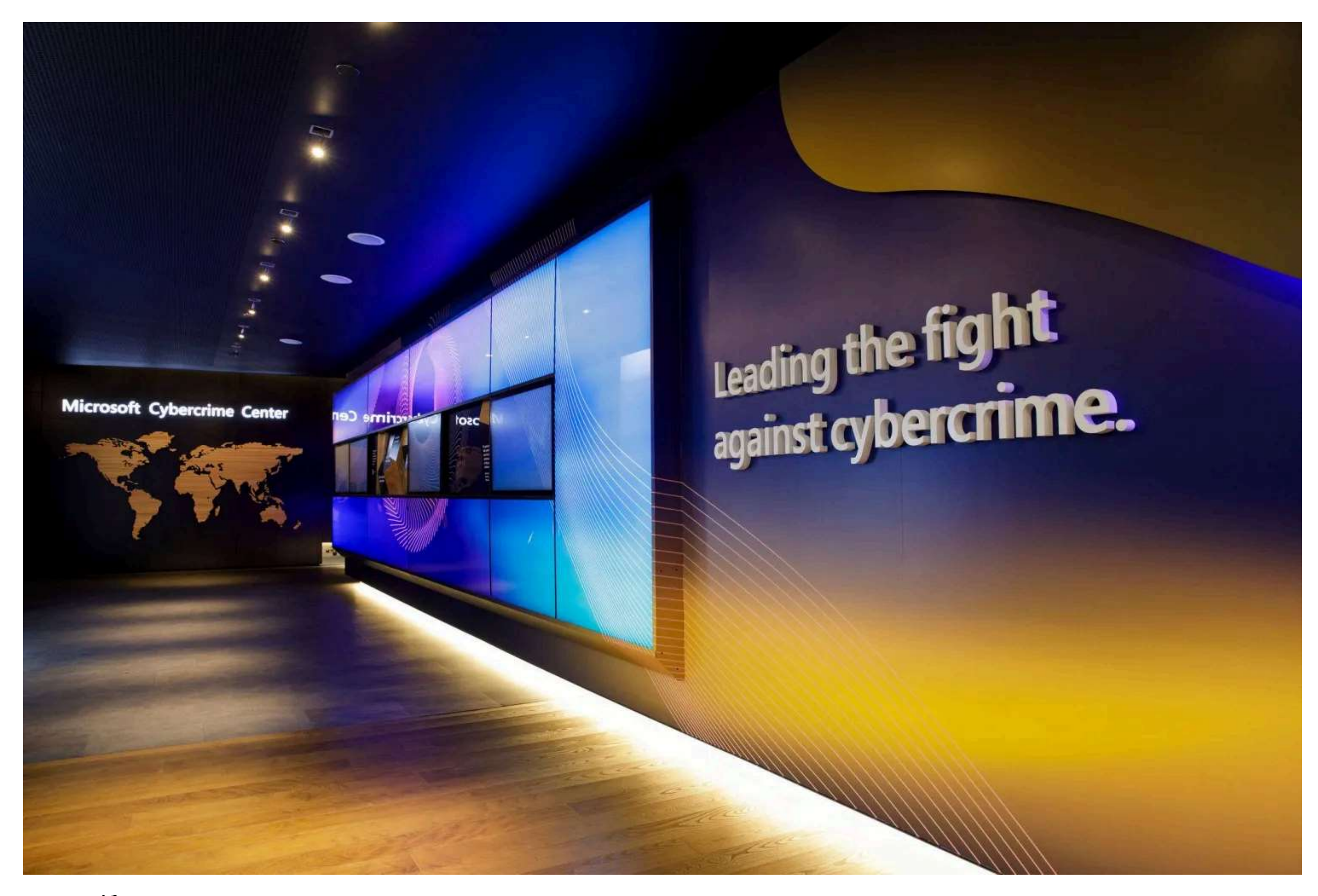
تكنولوجيا

## زيارة خاصة لـ«الشرق الأوسط» إلى «وحدة الجرائم الرقمية» في «مايكروسوفت»

# تحلل الوحدة 78 تريليون إشارة أمان يومياً بمساعدة الذكاء الاصطناعي




«مايكروسوفت»: نحن لا نتفاعل فقط مع التهديدات الإلكترونية بل نلاحق المجرمين ونفكك شبكاتهم ونجعل الإنترنت مكاناً أكثر أماناً للجميع (مايكروسوفت)

سياتل - الولايات المتحدة: نسيم رمضان

آخر تحديث: 16:27-31 يناير 2025 م . 01 شَعبان 1446 هـ
نُشر: 19:25-30 يناير 2025 م . 30 رَجب 1446 هـ

تُعتبر وحدة الجرائم الرقمية (DCU) التابعة لـ«مايكروسوفت» قوة حاسمة في المعركة العالمية الشرسة ضد الجرائم الإلكترونية. تقع هذه الوحدة في المقر الرئيسي للشركة في مدينة سياتل الأميركية، وتتبع نهجاً متعدد التخصصات يجمع بين الخبرة القانونية والتكنولوجيا المتطورة والشراكات العالمية لمكافحة بعض أكثر التهديدات الإلكترونية تطوراً في العالم. أتيحت لـ«الشرق الأوسط» زيارة حصرية لهذا المركز لرؤية كيفية عمل هذا الفريق المتخصص عن كثب، واستكشاف أحدث ابتكاراتهم، وفهم المشهد المتطور للأمن السيبراني.



ستيفن ماسادا المستشار العام المساعد لوحدة الجرائم الرقمية في «مايكروسوفت» (ستيفن ماسادا)

## محاربة الجرائم الإلكترونية

يقود هذه العمليات ستيفن ماسادا، المستشار العام المساعد لوحدة الجرائم الرقمية في «مايكروسوفت»، الذي يتمتع بخبرة واسعة من عمله السابق في وزارة العدل الأميركية، حيث قضى أكثر من 12 عاماً في التعامل مع ملاحقات وتحقيقات الجرائم الإلكترونية.



ويوضح ماسادا أن «مهمة المركز بسيطة ولكنها طموحة، وهي تعطيل عمليات المجرمين الإلكترونيين، وجعل العالم الرقمي أكثر أماناً للجميع».

تعمل وحدة الجرائم الرقمية منذ عام 2008، وشهدت تطوراً لتصبح شبكة عالمية تضم محامين ومحققين ومحللي بيانات ومحترفين في مجال الأمن السيبراني. يستفيد الفريق من شبكة استخبارات التهديدات الواسعة لـ«مايكروسوفت»، حيث يحلل 78 تريليون إشارة أمان يومياً بمساعدة الذكاء الاصطناعي لتتبع وتحييد التهديدات الإلكترونية قبل أن تتصاعد.

يقول ماسادا في حديثه لـ«الشرق الأوسط» إن «الجرائم الإلكترونية لم تعد مجرد أفراد يعملون بشكل منفرد بل أصبحت صناعة». ويضيف: «يعمل القراصنة مثل الشركات، حيث يقدمون الجرائم الإلكترونية بوصفها خدمة، مما يخلق سلسلة توريد من التهديدات الرقمية».

## غرفة محاكاة الجرائم الإلكترونية

عندما دخلنا إلى مركز مكافحة الجرائم الإلكترونية في «مايكروسوفت» تعرفنا على مساحة تجمع بين التحليل الجنائي واستخبارات التهديدات في الوقت الفعلي وجهود إنفاذ القانون.

كانت إحدى التجارب الأكثر إثارة هي زيارة غرفة محاكاة الهجمات الإلكترونية، حيث تتم إعادة بناء سيناريوهات الجرائم الإلكترونية الواقعية. يشرح ماسادا أن هذه المساحة تسمح للشركات والمسؤولين الحكوميين والمحترفين في مجال الأمن السيبراني بتجربة كيفية حدوث هجوم الفدية في الوقت الفعلي. تقدم المحاكاة التي اختبرناها تجربة تفاعلية تهدف إلى مساعدة الزوار على فهم التأثير الفوري للاختراق الإلكتروني واستراتيجيات الاستجابة اللازمة.



خلال عام 2024 ساهمت وحدة الجرائم الرقمية في 85 عملية اعتقال على مستوى العالم (شاترستوك)

## مختبر التهديدات والتحقيقات

في مختبر التحقيقات، يعمل المحللون الجنائيون وعلماء البيانات في «مايكروسوفت» على تتبع شبكات المجرمين الإلكترونيين. باستخدام التحليلات المدعومة بالذكاء الاصطناعي، يراقب الفريق أكثر من 3000 جهة تهديد إلكتروني معروفة عالمياً، بما في ذلك مجموعات تابعة لدول وشبكات الفدية وشبكات الاحتيال المالي. يسعون من ذلك إلى تحديد وتتبع وتعطيل عمليات المجرمين الإلكترونيين قبل أن تتسبب في ضرر.

يقول ماسادا إن العمل لا يقتصر على الاستجابة للتهديدات الإلكترونية، بل يتضمن أيضاً تفكيك البنية التحتية التي تمكنها بشكل استباقي.

وعلى طول الممرات، تعرض عدة أكشاك تفاعلية حالات رئيسية للجرائم الإلكترونية تمكنت وحدة الجرائم الرقمية (DCU) من تعطيلها بنجاح. تسلط هذه الحالات الضوء على جهود مايكروسوفت في إزالة أدوات التصيد الاحتيالي، وإيقاف عمليات الفدية، ومنع مخططات سرقة الهوية التي استهدفت ملايين المستخدمين حول العالم.

## حقائق

**13.82 تريليون دولار**

**هو حجم التكلفة العالمية للجرائم الإلكترونية بحلول عام 2028 بعد أن كانت 9.22 تريليون دولار في عام 2024**

### القانون لمكافحة الجرائم الإلكترونية

بينما تركز غالبية المنظمات فقط على الأمن السيبراني الدفاعي، تأخذ وحدة الجرائم الرقمية في «مايكروسوفت» نهجاً هجومياً باستخدام الاستراتيجيات القانونية لإيقاف شبكات المجرمين الإلكترونيين.

يوضح ماسادا أن «مايكروسوفت» تستخدم القانون أداة لتعطيل الجرائم الإلكترونية. من خلال الحصول على أوامر قضائية، يمكن مصادرة النطاقات وحظر الخوادم الخبيثة وتفكيك البنية التحتية الإجرامية.

وقد أثبت هذا النهج القانوني فاعليته الكبيرة في تعطيل الجرائم الإلكترونية ذات الدوافع المالية وحتى الجهات التابعة للدول. على مر السنين، قامت «مايكروسوفت» بمبادرات قانونية ضد بعض أخطر شبكات المجرمين الإلكترونيين في العالم، غالباً بالتعاون مع الحكومات ووكالات إنفاذ القانون وشركات الأمن السيبراني.

ومن أبرز الحالات تلك التي تتعلق بشبكة «ستورم - 1152» البارزة في عالم الجريمة الإلكترونية التي كانت تعمل على تطوير أداة مدعومة بالذكاء الاصطناعي لتجاوز إجراءات أمان «CAPTCHA» وإنشاء حسابات وهمية على نطاق واسع. تمكنت «مايكروسوفت» بالشراكة مع «أكروس لابس» من إيقاف هذه العملية، مما أدى إلى تقليل عدد الحسابات الوهمية بشكل كبير. ويعد ماسادا أن «المجرمين الإلكترونيين يتطورون باستمرار، ولكننا نتطور معهم».



يعمل في وحدة الجرائم الرقمية 34000 مهندس أمني متخصص بدوام كامل (شاترستوك)

## الذكاء الاصطناعي ومستقبل الجرائم الإلكترونية

أحد التحديات الأكثر إلحاحاً التي تواجهها وحدة الجرائم الرقمية اليوم هو إساءة استخدام الذكاء الاصطناعي التوليدي من قبل المجرمين الإلكترونيين. مع تقدم تقنيات الذكاء الاصطناعي بسرعة، يجد القراصنة طرقاً لاستغلالها في حملات التصيد الآلية، وكذا عمليات الاحتيال باستخدام «التزييف العميق» وسرقة الهوية.

خلال الجولة، تعرفت «الشرق الأوسط» على تحقيق حديث لـ«مايكروسوفت» كشف عن مجموعة إجرامية تستخدم محتوى تم إنشاؤه بالذكاء الاصطناعي لنشر المعلومات المضللة وتنفيذ مخططات الاحتيال. ردت وحدة الجرائم الرقمية من خلال إيقاف البنية التحتية الرقمية للشبكة. أيضاً عبر تحليل التهديدات المولدة بالذكاء الاصطناعي لتحسين دفاعات مايكروسوفت الأمنية والتعاون مع وكالات إنفاذ القانون لتتبع ومقاضاة المتورطين.

يؤكد ماسادا أن «الذكاء الاصطناعي أداة قوية، ولكن في الأيدي الخطأ، ويمكن أن يتم تحويلها إلى سلاح». لهذا السبب تستخدم «مايكروسوفت» الذكاء الاصطناعي ليس فقط لمكافحة الجرائم الإلكترونية، بل أيضاً لتوقعها ومنعها. وقد قامت وحدة الجرائم الرقمية بدمج أنظمة استخبارات التهديدات المدعومة بالذكاء الاصطناعي لفحص أنماط الأنشطة الإجرامية الإلكترونية، مما يساعد «مايكروسوفت» على توقع التهديدات الإلكترونية والتخفيف منها قبل حدوثها.

### جبهة موحدة ضد الجرائم الإلكترونية

أحد الدروس الرئيسية من الزيارة كان كيفية تعاون «مايكروسوفت» مع الحكومات وشركات الأمن السيبراني الخاصة ووكالات إنفاذ القانون لتعزيز تأثيرها. تتعاون وحدة الجرائم الرقمية بنشاط مع مكتب التحقيقات الفيدرالي (FBI) والإنتربول لتتبع المجرمين الإلكترونيين الدوليين. هناك أيضاً تنسيق مع شركات أخرى مثل «غوغل» و«أمازون» لاتخاذ إجراءات قانونية مشتركة ضد شبكات الاحتيال واسعة النطاق. إضافة إلى الحكومات المحلية.

كانت زيارة وحدة الجرائم الرقمية في «مايكروسوفت» تجربة مثيرة للتفكير سلطت الضوء على حجم وتعقيد الجرائم الإلكترونية الحديثة. كما يبدو أن ما يميز «مايكروسوفت» من خلال هذه الوحدة هو نهجها الاستباقي الذي يجمع بين استخبارات التهديدات المدعومة بالذكاء الاصطناعي وإنفاذ القانون والشراكات العالمية لمكافحة الجرائم الإلكترونية من جذورها.

